Pymes y autónomos, más **VULNERABLES** a los ciber ataques

El aumento de ciber ataques a las pymes y autónomos ha contribuido a aumentar su sensación de vulnerabilidad. La realidad es que esta crisis ha actuado como acelerador en la toma de conciencia de los riesgos cibernéticos que pueden paralizar su actividad. Eso se puede evitar transfiriendo gran parte de estos riesgos a una póliza de seguros que ofrecen soluciones en varios aspectos: ayudan a evaluar sus sistemas; si ocurre algo, proporcionan un asesor profesional que facilita la toma de decisiones y la evaluación de las consecuencias; y, si finalmente se incurre en perjuicios económicos, el seguro permite recuperar esos gastos y pagos.

El Covid-19 ha traído una transformación digital en el mundo empresarial, tanto a nivel organizativo, con el trabajo en remoto, como en el negocio online, que han ganado mucho peso. Todo eso ha llevado a un aumento de la probabilidad de sufrir un ataque cibernético y a hacernos más conscientes de la necesidad de establecer medidas para proteger nuestros sistemas y la conexión de los empleados desde su casa. El 'Informe Siniestros Ciber Hiscox 19', indica que entre los meses de abril y junio (en el punto más alto de reducción de la movilidad), el fraude financiero online creció un 67% y se dispararon las frecuencias de los ataques de *ransomware* (secuestro de datos). "Toda empresa que esté conectada con otra, puede servir de entrada para un ataque, y los ciberdelincuentes saben que es más sencillo atacar una pyme, porque dispone de menos recursos, para acceder después a una gran compañía", señala Alan Abreu, responsable de riesgos ciber de **Hiscox**. Así lo atestigua María Ameijeiras, directora general en **AyF Correduría de Seguros:** "las pymes y los autónomos tienen un nivel de seguridad menor y los ciberdelincuentes saben que es más fácil atacarlas. Tienen que invertir menos esfuerzo para hacerlo y, además, hay muchas más con las que intentarlo. En España, el 98% del tejido empresarial son pymes y estas representan el 60% de las empresas atacadas. El problema es que una gran parte de ellas tienen que cerrar después de haber sufrido un ataque".

Cristina Llorens, directora de Madrid de Negocios Estratégicos del **Instituto de Desarrollo Asegurador**, explica que "los datos están más en juego que nunca y los delincuentes lo saben. Es estremecedor ver cómo los cibercriminales se aprovechan de las necesidades sociales y cómo ha ido cambiando el escenario de los ataques informáticos en función de la evolución del Covid". En este sentido, Olivier Marcén, Financial Lines Leader Barcelona Branch CyberEdge Iberia Product Leader de **AIG**, comenta que "en los últimos meses hemos constatado la sofisticación, proliferación y personalización de algunos cibertataques".

El 70% de los ciberataques en España son a pymes, porque cuentan con menos protocolos de ciberseguridad que una empresa grande

MÁS EXTORSIONES EN PYMES

Aunque cualquier empresa, del tamaño que sea, puede padecer un ataque informático, en las pymes y autónomos existe menos conciencia de que pueden sufrirlo. Algo que, según Julio de Santos, presidente del Grupo **Alkora**, comienza a remitir porque "las empresas cada vez están sufriendo más extorsiones, intentos de estafa o secuestros de sus sistemas y el boca a boca, ha contribuido a aumentar la sensación de vulnerabilidad".

Pero Sergio Rueda, director de **Benjumea**, no lo tiene tan claro: "Hay pymes y autónomos que sí apuestan por la prevención, y otros no. Estos últimos seguramente desaparecerán del mercado, ya que la cuestión digital es básica hoy en día". En opinión de Cristina Llorens (Instituto de Desarrollo Asegurador), "faltan mensajes claros para hacer entender cuál es el riesgo que están corriendo las empresas y lo que podemos hacer por su seguridad".

José Ignacio Aguera, director de TIC de **CenterBrok**, piensa que "el día a día consume nuestro

SANCIONES POR NO TOMAR LAS MEDIDAS DE CIBERSEGURIDAD ADECUADAS

Las sanciones desde que se ha implantado el nuevo reglamento de protección de datos en el año 2018, se han endurecido:

- **Infracción menos grave: multas que pueden alcanzar hasta 10 millones de euros o el 2% del volumen de facturación anual de la empresa (la más alta de las dos).**
- **Infracción muy grave: multas que pueden alcanzar hasta 20 millones de euros o el 4% del volumen de facturación anual de la empresa (la más alta de las dos).**

Estas sanciones las puede imponer la Agencia Española de Protección de Datos (AEPD) por entender que la empresa no ha implementado las medidas suficientes en materia de seguridad.

Como señala Cristina Llorens (Instituto de Desarrollo Asegurador), "son sanciones cuantiosas y pueden llevarse por delante la viabilidad de la empresa". Sergio Rueda (Benjumea) añade que "la mayor sanción es la falta de credibilidad del operador y la fuga de clientes". Alan Abreu (Hiscox), afirma que "en torno al 60% de las pymes que sufren una brecha de seguridad grave, y no tiene seguro, desaparecen en los siguientes 6 meses". Por eso, María Ameijeiras (AyF Correduría de Seguros) dice que "es importante que se realice un análisis y gestión de riesgos para identificar todas las vulnerabilidades a las que pueden estar expuestos nuestros sistemas de información y establecer las salvaguardas y controles adecuados para minimizar el riesgo. Para ello existen metodologías como Magerit (Gobierno de España con su herramienta Pilar), Cramm, Cobra, etc. y también puede servir de ayuda para las pequeñas y medianas empresas la guía práctica de análisis de riesgos en los tratamientos de daños personales sujetos al RGPD para saber determinar en qué tipos de tratamiento se requiere una evaluación de impacto (EIPD)".

José Ignacio Aguera (CenterBrok) piensa que "sería interesante establecer y exigir protocolos de ciberseguridad más allá de los que establece la propia ley o reglamento de protección de datos. Es decir, proteger la presencia digital mediante el establecimiento de normativas al respecto (sistemas de ciberseguridad, firewalls de calidad, protocolos de uso empresarial para las herramientas digitales, etc.)".

tiempo, y en muchas ocasiones no analizamos los riesgos por ciberataques como un problema prioritario, eso redunda en una falta de concienciación global en la empresa. Por eso insisto en que la formación y la necesidad de disponer de asesoramiento profesional, debe ser un objetivo prioritario a nivel empresarial".

LOS RIESGOS DEL TELETRABAJO

Con el Covid 19, muchas empresas están optando por consolidar el modelo de teletrabajo. Esto implica una exposición mayor al riesgo de ataques informáticos. Esta crisis ha actuado como acelerador en la toma de conciencia sobre los riesgos cibernéticos y se ha convertido en una de las prioridades de las pymes, porque es algo que puede paralizar

su actividad. Por eso, muchas aseguradoras han reaccionado y han acomodado su condicionado de seguros a esta nueva realidad, incluyendo coberturas específicas que contemplan el teletrabajo.

En opinión de Sergio Rueda (Benjumea), "el teletrabajo es una oportunidad para robar credenciales. Una vez conseguido, se puede provocar una eventual denegación de servicio, la infección por *ransomware*…".

Los principales riesgos a los que se exponen las empresas son los daños en los sistemas informáticos del asegurado, la transmisión de malware a terceros, el incumplimiento del deber de custodia de datos de carácter personal, la interrupción de negocio, las sanciones y el daño reputacional. El seguro puede cubrir desde un error humano que propicia la divulgación de información propia o de terceros, hasta una fuga de información intencionada, el impacto en el negocio en caso de que un proveedor sufra un incidente que te afecte a ti, la negación de entrada en tu sistema por ataque informático que te impide continuar con tu actividad, incumplir normativas relacionadas con el deber de protección de la información, etc.

BLANCO DE LOS HACKERS

El 70% de los ciberataques en España son a pymes, porque cuentan con menos protocolos de ciberseguridad que una empresa grande y se convierten a menudo en blanco de los hackers. Los ciber ataques están catalogados como el tercer delito más extendido en el mundo, sólo lo supera el tráfico de drogas y la prostitución. De hecho, es 9 veces más probable sufrir un incidente cibernético, que un robo en nuestra oficina. España, actualmente, es el tercer país del mundo en número de ciberataques y esta situación está creciendo de forma exponencial día a día.

Los ciber ataques están catalogados como el tercer delito más extendido en el mundo, sólo lo supera el tráfico de drogas y la prostitución

Olivier Marcén (AIG), explica que "los ataques cada vez son más personalizados, lo que puede implicar periodos más extensos de paralización de la actividad y, en consecuencia, mayores pérdidas económicas. Esto se puede evitar transfiriendo gran parte de estos riesgos a una póliza de seguros que pueden incluir formación para empleados y análisis de vulnerabilidades. Asimismo, con la cobertura de primera respuesta, se ofrece atención 24 horas los 365 días del año".

Julio de Santos (Grupo Alkora) apunta que "los seguros de ciberrriesgos ofrecen soluciones en varios aspectos, primero ayudan a las pequeñas empresas y autónomos a tomar conciencia y evaluar sus sistemas, lo que permite la prevención. Si ocurre algo, incluso cuando sólo se tiene la sospecha, sirven para tener un asesor profesional que nos ayude a tomar decisiones y evaluar consecuencias. Por último, si finalmente se incurre en perjuicios económicos, el seguro ayuda a recuperar esos gastos y pagos".

Laura Lora, técnico superior en Responsabilidad Civil de Reale, dice que "con independencia de que los empresarios apliquen todas las medidas necesarias para evitar el ciberataque, nunca son suficientes y el riesgo siempre existe. Por eso, tener contratada una póliza de seguro ayuda a prevenir y minimizar los riesgos y, en caso de producirse el siniestro, permite mitigarlo".

María Ameijeiras (AyF Correduría de Seguros) recuerda que "las aseguradoras, sin unos requisitos mínimos en materia de seguridad, no acceden a asegurar".

Laura Lora (Reale) alerta de que "no todos los seguros Ciber que hay en el mercado son iguales, ni tampoco las necesidades de cada empresa. Por eso, es conveniente contratar un seguro especializado que se adapte a las circunstancias de cada compañía". Para encontrar la mejor opción es bueno contar con la ayuda de un corredor de seguros, porque las necesidades de cada pyme son totalmente distintas y dependiendo de ellas, se deben seleccionar unas coberturas u otras. Por eso, Sergio Rueda (Benjumea) afirma que junto "a un profesional especializado, se podrá asesorar sobre las necesidades específicas que tiene y ajustar el coste de la póliza".

Entre los meses de abril y junio (en el punto más alto de reducción de la movilidad), el fraude financiero online creció un 67% y se dispararon las frecuencias de los ataques de *ransomware*

TRABAJADORES INCAUTOS

Partiendo de la premisa de que la seguridad total no existe, porque las ciber amenazas están en constante evolución, se aconseja realizar evaluaciones regulares de vulnerabilidad, invertir en seguridad incluyendo la prevención y, dentro de ella, la formación y concienciación de los empleados para evitar los ataques, ya que el factor humano está detrás de cualquier brecha de seguridad. Olivier Marcén (AIG) afirma que "hay criminales especializados en ciber delincuencia que usan técnicas para engañar a los empleados, para intentar acceder a los sistemas de las empresas".

Uno de los riesgos más importantes proviene de acciones voluntarias o involuntarias de los empleados. Por eso, existe una cobertura llamada '*crime*' que es opcional y que protege, "del robo de los datos, incluyendo la infidelidad de empleados. Pueden cubrir la perdida por un fraude de documentos, fraude electrónico o telefónico e incluso una extorsión", indica Cristina Llorens (Instituto de Desarrollo Asegurador). Esta cobertura responde cuando el empleado de una compañía es engañado por un (tercero) supuesto proveedor, directivo o compañero de empresa a través de correo electrónico, SMS o voz, con la intención de robar o modificar información valiosa para defraudar.

Normalmente, dice Julio de Santos (Grupo Alkora), "se incluyen los gastos de investigación y el propio rescate de la información, en caso de que se hubiese producido. También existen otras coberturas más novedosas, como el robo de fondos de la sociedad por un ataque cibernético o por suplantación de identidad".

La cultura de la ciberseguridad en las pymes españolas es todavía reactiva. Tan solo un 36% de las pequeñas y medianas empresas encuestadas tiene establecidos protocolos básicos de seguridad. Apenas un 14% de ellas actualiza sus contraseñas y sólo un 21% hace regularmente copias de seguridad. El coste medio de un ciberataque a una pyme es de 35.000 euros y el 60% cierra después de haberlo sufrido.

En las previsiones de Hiscox, a principio de año, ya apuntaban que los ataques *ransomware* continuarían

castigando al tejido empresarial. El secuestro de información sensible mediante el uso de software malicioso puede causar grandes pérdidas a las empresas, tanto en el campo reputacional como en lo que a dinero se refiere. Los seguros siempre recomiendan no pagar el rescate para liberar los datos de la empresa, ya que es un gesto que incentivará a otros ciberdelincuentes a volver a atacarle. Se prefiere estudiar la gravedad del "secuestro" y las posibilidades de recuperación antes de tomar la decisión del pago. Pero, si llegado el momento hubiera que hacerlo, la póliza de Ciberriesgo asumiría el coste del rescate.

REDUCIR EL TIEMPO DE RECUPERACIÓN

José Ignacio Aguera (CenterBrok) explica que "debido a la complejidad y variedad de los ataques, no existen reglas fijas para determinar los períodos de recuperación. Pueden extenderse a varios meses, porque el daño no es sólo económico o de pérdida de información, existe un alto riesgo por deterioro de imagen empresarial, que puede provocar un daño severo en la actividad digital de pequeñas empresas, en algunos casos irreversible".

Según el 'Informe de Ciberpreparación 2020' de Hiscox, tras descubrir una brecha de seguridad, la recuperación es más rápida en micro y pymes, ya que a las 5 horas, el 50% de ellas han recuperado su actividad habitual. En esta fase, influye mucho la dimensión de la compañía y la complejidad de sus sistemas. En estos casos, es importante disponer de una póliza para riesgos Ciber por el servicio de respuesta inmediata: con una llamada se pone en funcionamiento un entramado de profesionales especializados en localizar y detener el ataque, para que no vaya a más.

COBERTURAS QUE NO DEBEN FALTAR EN UN CIBERRIESGO

El seguro Ciber debe incluir, entre otras cosas:

- **Servicios de prevención (que tenga formación y análisis de madurez cibernética), de acompañamiento y asesoramiento al cliente.**
- **Fugas de datos, en la que se accede a la información comercial sin autorización (de manera electrónica o de otra forma).**
- **Ataques cibernéticos, cualquier ataque digital contra tu negocio.**
- **Extorsión, cibercriminales que secuestran tus sistemas o datos extorsionándote o amenazándote que van a publicar información.**
- **Errores humanos, errores cometidos por empleados o proveedores que desencadenan una brecha de datos o un fallo en la seguridad.**
- **Interrupción del negocio, la pérdida de beneficios por el ataque cibernético.**
- **Reglamento General de Protección de Datos, cubre tu responsabilidad y el coste de defensa por investigaciones regulatorias tras una brecha de datos, incluso sanciones por incumplimiento voluntario.**
- **Fraude y crimen financiero, el uso de Internet para engañar a empleados, empresas, clientes o proveedores para que hagan transferencias monetarias o de mercancías falsas.**
- **Servicio de Respuesta a Incidentes 24/7 para el restablecimiento de los sistemas y recuperación de datos de tu empresa a través de consultoras especializadas en asistencia informática, legal o de comunicación.**
- **Reclamaciones por contenido digital, derivadas de un ataque a tu página web o redes sociales que suponga un incumplimiento del derecho de propiedad intelectual o difamación (calumnia o menosprecio hacia un producto o competidor).**
- **Paralización de los sistemas del proveedor tecnológico. En caso de que tu proveedor tecnológico sufra un incidente y esto te impida trabajar.**
- **Gastos de emergencia y Pagos PCI-DSS (cuando gestiona plataforma de pagos).**
- **Cobertura de los daños reputacionales.**

María Ameijeiras, directora general en AyF Correduría de Seguros, dice que "es muy importante analizar si cubren las sanciones y los gastos de defensa por incumplimiento involuntario en materia de protección de datos, y revisar los límites de estas garantías porque hay diferencias entre unas soluciones y otras".

Hay que tener en cuenta que, habitualmente, los proveedores tecnológicos externalizados no están incluidos en las pólizas de las empresas. Por eso, existe la cobertura de Proveedor Externo de Servicio que cubre la pérdida de beneficio que sufre una empresa como consecuencia de un fallo de seguridad por parte de este proveedor y que provoca que no pueda prestar sus servicios. Olivier Marcén (AIG) entiende que "es una cobertura muy importante, dado el número de servicios tecnológicos subcontratados hoy en día y la enorme dependencia de ellos".

De la misma opinión es Julio de Santos (Grupo Alkora): "en las pymes estos servicios externalizados funcionan como un departamento más

ANTE LA AMENAZA DEL OTRO VIRUS INVISIBLE, CUALQUIER EMPRESA PODRÍA SUFRIR UN CIBERATAQUE

¿Sabrías cómo protegerte?

Te ofrecemos la **solución más completa** frente a cualquier amenaza digital.

Contacta con nosotros:

Protege tu ciber

Instituto de Desarrollo Asegurador

www.protegetuciber.com

www.iddeas.eu

de la empresa, trabajan con los datos de la compañía y sus sistemas garantizan la continuidad de negocio, por lo que, sin duda, es fundamental que las pólizas tengan en cuenta a estos proveedores en sus coberturas, como una parte más de la propia empresa".

EL RIESGO CIBERNÉTICO ES EL MÁS IMPORTANTE PARA UNA EMPRESA

Parece que la concienciación ha crecido rápidamente en los últimos tiempos. Julio de Santos (Grupo Alkora), dice que "en nuestra experiencia las pymes, muchas de ellas sin un departamento interno de informática, tienen más necesidad de tener alguien a quien dirigirse en caso de sufrir un incidente de estas características y saber cómo están en materia de seguridad. Sus necesidades, en este momento, se encuentran más en el terreno de la prevención. De hecho, hemos visto la respuesta reciente de algunas aseguradoras incluyendo servicios de prevención".

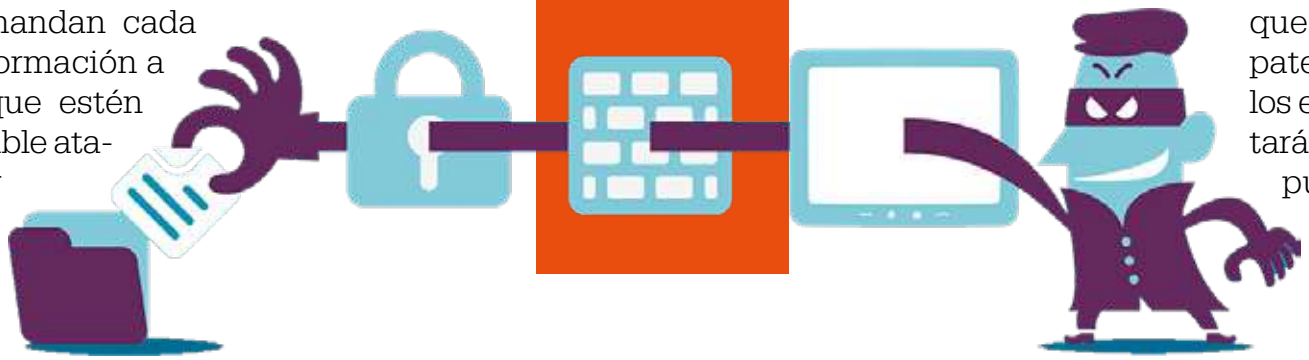
Cristina Llorens (Instituto de Desarrollo Asegurador) coincide en que "la mayor necesidad que demandan las pymes son el asesoramiento y servicio. Soluciones rápidas y eficaces a sus problemas y las buenas pólizas de Ciberriesgo lo incluyen".

Laura Lora (Reale Seguros) incide en que "a día de hoy las empresas demandan cada vez más una mayor información a sus empleados para que estén preparados ante un posible ataque, unido a un mayor asesoramiento en los riesgos de su empresa y un servicio de prevención que las acompañe desde el momento de contratación de la póliza".

El coste medio de un ciberataque a una pyme es de 35.000 euros y el 60% cierra después de haberlo sufrido

María Ameijeiras (AyF Correduría de Seguros) indica que "a nosotros lo que más nos están demandando es la cobertura de pirateo de fondos que, aunque no están todas las aseguradoras dispuestas a dar esta cobertura, si tenemos solución. Por otro lado, empieza a preocupar mucho en la industria la posibilidad de una parada por hackeo a máquinas. Cada vez hay más procesos automáticos y más robots también autómatas, el desarrollo del internet de las cosas está poniendo de relieve sus vulnerabilidades y el aumento de los ataques por esta vía. En este sentido, es fundamental hacer un análisis profundo de los condicionados, de las cláusulas y definiciones de las distintas soluciones aseguradoras antes de elegir y aquí es dónde entiendo que los corredores especialistas en este tipo de riesgos podemos aportar un gran valor".

La realidad, explica Alan Abreu (Hiscox), es que "las peticiones de cotizaciones para este seguro no han parado de crecer en todo el año, sin duda la transformación digital ha impulsado el negocio de estas pólizas". Cristina Llorens (Instituto de Desarrollo Asegurador) cree que "mucho más importante que mantener sus activos tangibles seguros, es el valor que tiene su marca, sus patentes y sus datos. Según los expertos, en 2021 aumentará en casi un 40% el presupuesto de ciberseguridad y no debe de faltar el seguro Ciber".



INFORMACIÓN RELEVANTE PARA PYMES Y AUTÓNOMOS

A DIARIO

Accede a las noticias que te interesan en:

WWW.PYMESEGUROS.COM